NEW BOUNDARY
TECHNOLOGIES®

Implementation of Commonly Accepted Security Configurations for Federal Agencies Using the XP Windows Operating System

A New Boundary Technologies
Security Configuration Guide

Based on OMB Memorandum M-07-11
and
NIST Special Publication 800-68

Table of Contents

1.0 Executive Summary

This Security Guide was developed by New Boundary Technologies to provide insight and recommended security configurations for federal agency CIO's and their network administrators who have been directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS) by 1 February 2008 for their Windows XP computers. Testing and analysis from the NSA and NIST have shown that establishing a common security configuration provides a baseline level of security, reduces risk from security threats and vulnerabilities, and saves time and resources. This will allow agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information.

Over the last few years, organizations including Microsoft, the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST), have developed guidance on securing Windows XP workstations within a variety of environments. The guidance offered by these organizations is based on consensus best practices for Windows client PC security. While perimeter defense measures remain an integral component of network security, many IT security experts and organizations have concluded that system lockdown (applying a security configuration template) now represents a primary opportunity for enhancing the overall security state of a network. This is especially true for organizations with heightened security requirements resulting from the nature of their organizational charter, such as government, intelligence, and military organizations, as well as enterprises with increased security concerns resulting from regulatory compliance requirements.

According to NIST, when a computer security configuration template (e.g., hardening or lockdown guide) is applied to a system, in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. In fact, actual testing by the NSA and NIST of these templates on workstations and servers has shown that they will reduce the vulnerabilities on systems by 80 to 90 percent. More recent testing by eWeek Labs shows that locking down a system running Windows XP SP2 to just "User Rights," showed no infections after visiting five websites known to install malware. Those same systems, with elevated rights to Administrator or Power User, experienced 16 infections each!

While system lockdown is not a new concept, it has always been an extremely time-consuming manual process, especially in a heterogeneous environment, because of the wide variety of different client PC configurations involved. Until the advent of Policy Commander®, there was no way to easily target individual computers or groups of computers based on configuration traits. Using Policy Commander, administrators can now implement security policies that lock down client PCs based on virtually any configuration trait, from operating system and service pack level to Windows services and even specific registry settings. For the first time, network and desktop administrators now have an automated solution that empowers them to quickly and easily implement security best practices for Windows XP via security policy enforcement and dynamic configuration management.

This guide is based upon the NIST High Security Level (which has recently has been renamed as Specialized Security-Limited Functionality) recommendations from the National Institute of Standards and Technology Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The complete version of 800-68 is available from NIST at: http://csrc.nist.gov/

2.0 Proactive Approach to Security Configuration Management

As Federal CIO's know, section 3544(b)(2)(D)(iii) of the Federal Information Security Management Act (FISMA) requires agencies to develop minimally acceptable system configuration requirements and ensure compliance with them. Federal agencies are already required to:

- Document in their annual FISMA report the frequency by which they have implemented system configuration requirements; and

- Use published configurations or be prepared to justify why they are not doing so.

The U.S. Air Force currently uses common security configurations for Microsoft Windows XP. These configurations were developed in collaboration with the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and Microsoft. These same organizations recently established common security configurations for Microsoft Windows Vista. With these common security configurations now in place, Federal Agencies have a unique opportunity to significantly increase the security of their computers using Microsoft Windows XP and Windows Vista.

Under the current OMB requirements, agencies must develop plans for Microsoft Windows XP and Vista that describe the following items:

- Testing configurations in a non-production environment to identify adverse effects on system functionality;
- Implementing and automating enforcement for using these configurations;
- Restricting administration of these configurations to only authorized professionals;
- Ensuring new acquisitions by June 30, 2007, to include these configurations and require information technology providers to certify their products operate effectively using these configurations;
- Applying Microsoft patches available from DHS when addressing new Windows XP or Vista vulnerabilities;
- Providing NIST documentation of any deviations from these configurations and the rationale for doing so; and
- Ensuring these configurations are incorporated into agency capital planning and investment control processes.

Locking down systems means that the user has no Administrator or Power User Rights within Windows XP and involves applying one of the security templates that have been developed over the years by NIST, NSA, DISA, and Microsoft. Locking down systems is a proactive way to combat the increasing threats from viruses, Trojan horses, and hidden root kits that exploit the security vulnerabilities exposed when a system has Administrator rights.

2.1 Lockdown Issues

If locking down systems is a proven way to increase the security of your workstations, then why hasn't it been more widely adopted? There are a number of reasons for the lack of widespread use of system lockdown. Aside from it not being popular with users who have had Administrator rights on their systems, the number one reason is that applying any lockdown security template can be a complex and time-consuming task that sometimes requires the use of numerous complex and separate tools for workstations and servers. In addition, locking down a workstation without thorough testing can cause unexpected interruptions in availability of applications and network resources. This can lead to productivity losses throughout the organization as end-users become unable to access mission critical applications or network resources.

Furthermore, once a system was locked down with a template or security baseline configuration, it was extremely hard to detect when a system became unlocked or non-compliant. When non-compliance was discovered, it was a manual process to remediate the system and bring it back into compliance. For these reasons network administrators tended to avoid applying the lockdown templates to their systems and thus have missed an opportunity to eliminate up to 90 percent of their systems vulnerabilities.

If you plan to lock down systems it is recommended that a multi-faceted approach be taken. You will still need good anti-virus, anti-spyware, firewall, VPN, patch management and software distribution solutions and the right framework and processes that will allow you to handle users' issues in a locked down environment. However, to eliminate the inherent vulnerabilities in default Windows XP configurations and implement proactive security configuration best practices, you will also need a good security policy management solution which automates and streamlines policy implementation, monitoring and enforcement. In fact, **"implementing and automating enforcement for using these configurations"** is a now a requirement per the OMB memorandum.

2.2 Policy Commander Approach

To address the need for a robust, easy to use security policy management solution, New Boundary Technologies developed Policy Commander™. Policy Commander eliminates the complexity of customizing, deploying, managing and maintaining security configurations and policies on desktops and servers. Policy Commander is a *single solution* that includes a growing library of proven best practices security policies that can be applied to both workstations and servers.

Policy Commander eliminates the need to learn how to use separate tools and scripting languages for different versions of Windows workstations and servers. The full NIST templates, especially those with more stringent security settings, can be challenging to implement and enforce without adversely affecting connectivity and application availability, and therefore require extensive testing. While Policy Commander includes policies based on the full NIST templates, in order to streamline testing requirements and provide a more granular security configuration methodology, we have also modularized the NIST templates into sets of Policy Commander security policies that are much easier to test, implement, and manage. New Boundary Technologies recommends that administrators assign and enforce the security policy modules derived from the NIST templates to incrementally harden a computer's security configuration, rather than assigning and enforcing the security policies based on the full NIST security templates. Incremental or granular hardening will significantly reduce the amount of time and effort required to test settings and their impact on applications and network connectivity, and minimize any loss of productivity with the organization.

Policy Commander is unique in its ability to precisely target security policies to the appropriate computers, which dramatically reduces the time and effort required to deploy security policies. Policy Commander is designed to continuously monitor the configuration state of computers and security policies, notify administrators of any instances of non-compliance, and automatically remediate those non-compliant computers. Policy Commander is a solution that significantly reduces the complexity, time, and effort to package, test, deploy, monitor and enforce any security policy on any Windows-based server or workstation located anywhere in your network worldwide.

Appendix A contains a chart that describes the security policies contained in the Policy Commander Security Policy Knowledge Base.

To request a full Policy Commander Evaluation version please contact New Boundary Technologies through our website at:
http://www.newboundary.com/products/policycommander/download.htm

3.0 New Boundary Technologies Lockdown Security Guide

The purpose of this guide is to show how Policy Commander can easily and quickly lock down Windows XP workstations and servers through application of the proven NIST Specialized Security-Limited Functionality template. This NIST template modifies several key policy areas of a Windows XP system, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions. The template is based on security templates previously developed by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and Microsoft. Most of the settings (198) in the template represent consensus recommendations as proposed by various security experts from the Center for Internet Security (CIS), DISA, NSA, Microsoft, and NIST.

While NIST has developed different template settings for use in SOHO, Legacy, Enterprise and High Security environments, NIST has recommended that any company that has to comply with regulatory security requirements such as HIPAA and SOX should look at using the XP Specialized Security-Limited Functionality template discussed in this guide. Therefore, New Boundary Technologies recommends that any federal agency workstations that are targeted to be locked down should use or be migrated to the Windows XP operating system. This will not only provide the highest level of security but significantly ease the task of testing, applying and maintaining the Specialized Security-Limited Functionality template for Windows XP.

3.1 High Security or Lockdown Environment

A high security or lockdown environment is any environment, networked or standalone, which is at high risk of attack or data exposure. This environment encompasses computers that contain highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting, payroll processing, air traffic control). These computers might be targeted by third parties for exploitation, but also might be targeted by trusted parties inside the organization. A high security environment could be a subset of a SOHO or Enterprise environment. For example, three desktops in an enterprise environment that hold confidential financial or customer data could be thought of as a high security environment within an enterprise environment. In addition, a laptop used by a mobile worker might be a high security environment within a SOHO environment. A high security environment might also be a self-contained environment outside any other environment – for instance, a government security installation dealing in sensitive data.

Systems in high security or locked down environments face threats from both insiders and external parties. Because of the risks and possible consequences of a compromise in a high security environment, it usually has the most restrictive and secure configuration. The suggested configuration provides the greatest protection at the expense of ease of use, functionality, and remote system management. In a high security environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

3.2 Best Practices for Analysis and Testing of Security Policies

Although the NIST security settings have undergone considerable testing and are recommended for companies looking to achieve the highest security configuration, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST Windows XP Specialized Security-Limited Functionality Template was driven by the need to create a more secure Windows XP workstation configuration. Because some settings in the templates may reduce the functionality or usability of the system, it is not recommended that the complete template be used as a baseline security configuration. Specific settings in the templates should be modified as needed so that the settings conform to local policies and support required system functionality. New Boundary Technologies strongly recommends that organizations fully test the security policies contained in Policy Commander on representative systems before widespread deployment. Some lockdown settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile. The value of Policy Commander is that is was designed to provide administrators with the flexibility and power to create tailored lockdown security configurations for their unique network needs and architectures.

New Boundary Technologies recommends the following steps be taken to test the policies:

1) **Analyze:** Conduct a risk assessment of the assets in your network. Use Policy Commander as part of the risk assessment to compare the current security policies of the local workstation/servers to the policies required to meet the high security standards.

2) Test: When new security settings or policies are applied, they can interfere with the operation of existing software applications and other operations on the target computers. We strongly recommend testing each new policy thoroughly in the test environment before moving it to the production environment.

- 2.1 System administrators build their systems from a clean formatted state to begin the process of securing Windows XP workstations.

- 2.2 The installation and test process should be performed on a secure network segment or off the organization’s network until the security configuration is completed.

- 2.3 All patches, service packs, hotfixes and rollups for XP are applied.

- 2.4 All desktop or server applications are installed, operational and have all upgrades/patches applied.

- 2.5 Strong passwords are set for all accounts.

3) **Assign:** Use Policy Commander to install the security policy modules in the test mode.

In the past, network administrators would have to apply the entire template and then spend hours troubleshooting the 198 settings to see which ones caused a problem on the test workstation. By reducing those 198 settings to a more manageable number of key policies, network administrators now can individually apply each policy, modify it if necessary, and then add the next policy. This will significantly decrease the time to test and configure the high security configuration that best fits your environment. Administrators will realize additional time saving from Policy Commander's unique ability to precisely target security policies to the appropriate computers or groups of computers.

The NBT Security Policies are organized based on the nine categories identified by NIST. Those categories are:

1) Account Policies
2) Local Policies
3) Event Log Policies
4) Restricted Groups
5) System Services
6) File Permissions
7) Registry Permissions
8) Registry Values
9) File and Registry Auditing

Appendix A provides an overview of these nine categories and which NBT Security Policies are in each category. Appendix B provides you with links to multiple security resources.

4) **Enforce:** Save final security configuration baseline, use Policy Commander to organize your key workstations and servers that will be locked down, and then deploy the Lockdown Security Configuration Baseline. New Boundary Technologies recommends that the automatic enforcement feature be utilized to ensure complete 24x7 enforcement of your lockdown configuration.

For a complete overview of how Policy Commander works download the 30 day evaluation at: *http://www.newboundary.com/products/policycommander/index.htm*.

4.0 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.

- Reduce the opportunities that attackers have to breach a system by limiting functionality according to the principle of least privilege and resolving security weaknesses (i.e. lockdown).

- Select security controls and policies that provide a reasonably secure solution while supporting the functionality and usability that users require.

- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.

- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.

- Document procedures for implementing and maintaining security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.

- Test all security controls, including the settings in the NIST security templates, to determine what impact they have on system security, functionality, and usability. Take appropriate steps to address any significant issues.

- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions include acquiring and installing software updates, monitoring event logs, providing remote system administration and assistance, monitoring changes to OS and software settings, protecting and sanitizing media, responding promptly to suspected incidents, performing vulnerability assessments, disabling and deleting unused user accounts, and maintaining hardware.

Appendix A

New Boundary Technologies Lockdown Security Policies

This chart describes the security policies authored by New Boundary Technologies based on setting recommendations contained in the Windows XP High Security Template. These policies are organized into nine key security categories based on the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The New Boundary Technologies policies contain the recommended settings from the NIST XP High Security Template but also include custom policies developed by NBT to meet unique security requirements not achievable using Microsoft Active Directory and Group Policies.

Security Categories	Policy Commander Policies
1.0 Account Policies	• Harden account lockout settings
2.0 Local Policies 2.1 Audit Policies 2.2 User Rights Assignment 2.3 Security Options	• Control the System Audit Policy settings • Harden the User Rights Assignment settings • Disable the Guest Account • Limit local account use of blank passwords to console only • Harden Device settings • Harden Domain Member settings • Harden Interactive Logon settings • Harden Microsoft network server settings • Harden network access settings • Harden network security settings • Harden Recovery Console settings • Harden Shutdown settings • Enforce FIPS Certified Cryptography • Harden System Objects settings • Shut down immediately if unable to log security audits • Disallow anonymous SID_Name translation • Force logoff when logon hours expire
3.0 Event Log Policies	• Control Event Log settings
4.0 Restricted Groups	• Remove all users from the Remote Desktop Users and Power Users groups.
5.0 System Services	• Alerter • Clipbook • FTP Publishing • HS Admin Service • Messenger • NetMeeting Remote Desktop Sharing • Routing and Remote Access • Simple Mail Transfer Protocol (SMTP) • Simple Network Management Protocol (SNMP) Service • SNMP Trap

	• Telnet • World Wide Web Publishing Services • Computer Browser • Remote Registry • Task Scheduler • Terminal Services • Fax Service • Indexing Service • Remote Desktop Help Session Manager • Universal Plug & Play Device Host • Netlogon
6.0 File Permissions	• Harden security permissions for critical files
7.0 Registry Permissions	• Harden security permissions for critical registry keys
8.0 Registry Values 8.1 Debugging 8.2 Automatic Functions 8.3 Networking	• Disable the Dr. Watson debugger and memory dump file • Disable automatically running CD-ROMs • Disable automatic administrator logon • Disable automatic reboot • Strengthen miscellaneous networking settings • Harden the Microsoft TCP/IP stack settings
9.0 Custom NBT Policies	• Policies that address unique infrastructure requirements
9.1 Automatic Logoff	• Policy that can be set to automatically log off a user after a set time limit.
9.2 Sensitive File Protection	• Policies that can restrict access to files or folders that contain sensitive or classified information to only those with authorized access.
9.3 USB Removable Device	• Policies that will prevent the attachment and/or use of portable USB storage devices.

Appendix B

Security Resources

B.1 Security Configuration Resources

The Microsoft Windows XP security configurations are at: http://csrc.nist.gov/itsec/download_WinXP.html, and the Microsoft Vista security configurations are at http://csrc.nist.gov/itsec/guidance_vista.html.

OMB's FISMA reporting instructions are located at: http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf.

Any security configurations developed by your agency for other operating systems should be sent to NIST at checklists@nist.gov. NIST will work with your agency to determine whether they can be published as common security configurations for use by other agencies.

There are now over 120 common security configurations published on NIST's web site. For more information, see: http://checklists.nist.gov. NIST's Computer Security Division website is located at http://csrc.nist.gov/. For more information about the security content automation program, see http://nvd.nist.gov/scap.cfm.

NIST Special Publication 800-70, "Security Configuration Checklist Program for IT Products," is located at http://csrc.nist.gov/checklists/SP800-70-DRAFT.pdf.

B.2 Vulnerability Databases

National Vulnerability Database (NVD)
http://nvd.nist.gov/

Open Source Vulnerability Database
http://www.osvdb.org/

SecurityFocus Vulnerability Database
http://www.securityfocus.com/bid/

United States Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database
http://www.kb.cert.org/vuls/

B.3 Mailing Lists

Microsoft Security Notification Service
http://www.microsoft.com/technet/security/bulletin/notify.mspx

SecurityFocus – BugTraq
http://www.securityfocus.com/archive/1

US-CERT National Cyber Alert System
http://www.us-cert.gov/cas/

B.4 Print Resources

Allen, Robbie and Gralla, Preston, *Windows XP Cookbook*, O'Reilly, 2005.
Bott, Ed, et al., *Microsoft Windows XP Inside Out, Second Edition,* Microsoft Press, 2004.
Bott, Ed and Siechert, Carl, *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press, 2002.
Boyce, Jim, *Windows XP Power Tools*, Sybex, 2002.
Honeycutt, Jerry, *Microsoft Windows XP Registry Guide,* Microsoft Press, 2002.
Moskowitz, Jeremy, *Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows XP, and Windows 2000*, Sybex, 2004.
Moulton, Pete, *SOHO Networking: A Guide to Installing a Small-Office/Home-Office Network*, Prentice Hall PTR, 2002.
Russel, Charlie and Crawford, Sharon, *Microsoft Windows XP Professional Resource Kit, Third Edition*, Microsoft Press, 2005.
Simmons, Curt and Causey, James, *Microsoft Windows XP Networking Inside Out*, Microsoft Press, 2002.
Thurrott, Paul, *Windows XP Home Networking, 2nd Edition*, John Wiley and Sons, 2004.
Weber, Chris and Bahadur, Gary, *Windows XP Professional Security*, McGraw-Hill, 2002.

B.5 Related NIST Documents and Resources

Computer Security Resource Center Special Publications
http://csrc.nist.gov/publications/nistpubs/index.html

SP 800-28, *Guidelines on Active Content and Mobile Code*
SP 800-30, *Risk Management Guide for Information Technology Systems*
SP 800-34, *Contingency Planning Guide for Information Technology Systems*
SP 800-40, *Procedures for Handling Security Patches*
SP 800-42, *Guideline on Network Security Testing*
SP 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*
SP 800-46, *Security for Telecommuting and Broadband Communications*
SP 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*
SP 800-53, *Recommended Security Controls for Federal Information Systems*
SP 800-61, *Computer Security Incident Handling Guide*
SP 800-70, *Security Configuration Checklists Program for IT Products*
SP 800-77, *Guide to IPsec VPNs*
SP 800-83, *Guide to Malware Incident Prevention and Handling*

FIPS Publications
http://csrc.nist.gov/publications/fips/index.html
FIPS 140-2, *Security Requirements for Cryptographic Modules*
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Draft Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems*

FISMA Implementation Project
http://csrc.nist.gov/sec-cert/
Security Checklists Program for IT Products project
http://csrc.nist.gov/checklists/
Security Configuration Checklists Repository for IT Products project
http://csrc.nist.gov/checklists/repository

B.6 Microsoft Web-Based Resources

Microsoft's Web site contains a wealth of information regarding Windows XP and Windows security. This section lists many of these resources, divided into five categories: general Windows XP resources, general security resources (i.e., not XP-specific), general and specific Windows XP security resources, and Microsoft knowledge base articles.

B.6.1 General Windows XP Resources

Features and Functionality in Windows XP Service Pack 2
http://www.microsoft.com/technet/prodtechnol/winxppro/plan/xpsp2ff.mspx

Microsoft Technet
http://www.microsoft.com/technet/

Microsoft Windows XP Professional Resource Kit Documentation
http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/enus/prork_overview.asp

Windows Application Compatibility
http://www.microsoft.com/windows/appcompatibility/default.mspx

Windows XP Home Page
http://www.microsoft.com/windowsxp/default.mspx

Windows XP Professional Features
http://www.microsoft.com/windowsxp/pro/evaluation/features.mspx

Windows XP Service Pack 2 Resources for IT Professionals
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx

Administering Group Policy with Group Policy Management Console
http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

Enterprise Management with the Group Policy Management Console
http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

B.6.2 General Security Resources

Microsoft Download Center
http://www.microsoft.com/downloads/search.aspx?displaylang=en

Microsoft Security Home Page
http://www.microsoft.com/security/

Microsoft Security Notification Service
http://www.microsoft.com/technet/security/bulletin/notify.mspx

Microsoft TechNet Security Resource Center
http://www.microsoft.com/TechNet/security/default.mspx

Microsoft Windows Update Web site
http://windowsupdate.microsoft.com/

Security Bulletins
http://www.microsoft.com/security/bulletins/alerts.mspx

Security Guidance Center for Developers and IT Pros
http://www.microsoft.com/security/guidance/default.mspx

Windows Server Update Services
http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

B.6.3 General Windows XP Security Resources

Group Policy Settings Reference for Windows Server 2003 with Service Pack 1
http://www.microsoft.com/downloads/details.aspx?FamilyID=7821c32f-da15-438d-8e48-45915cd2bc14&displaylang=en

Home and Small Office Networking with Windows XP
http://www.microsoft.com/windowsxp/using/networking/default.mspx

Securing Mobile Computers with Windows XP Professional
http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/mblsecxp.mspx

Step-by-Step Guide to Securing Microsoft Windows XP Professional in Small and Medium Businesses
http://www.microsoft.com/windowsxp/using/security/learnmore/smbsecurity.mspx

Threats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP
http://www.microsoft.com/downloads/details.aspx?FamilyId=1B6ACF93-147A-4481-9346-F93A4081EEA8&displaylang=en

What's New in Security for Windows XP Professional and Windows XP Home Edition
http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/xpsec.mspx

Windows XP Baseline Security Checklists
http://www.microsoft.com/technet/security/chklist/xpcl.mspx

Windows XP Security Guide v2.0 (updated for Service Pack 2)
http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx

B.6.4 Specific Windows XP Security Topics

Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

Data Protection and Recovery in Windows XP
http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspx

Don't Let the Defense Rest: Securing Home Networks with Windows XP
http://www.microsoft.com/windowsxp/using/networking/expert/bowman_november12.mspx

Enabling the Startup Key
http://www.microsoft.com/resources/documentation/windows/xp/all/reskit/enus/
prnb_efs_zbxr.asp

Encrypting File System in Windows XP and Windows Server 2003
http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx

Features Available on NTFS Volumes
http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/enus/
prkc_fil_gywp.asp

Get Started Using Remote Desktop
http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx

How to Set Up and Use Automated System Recovery in Windows XP
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/asr.mspx

How to Share Files Using Encrypting File System
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sharefilesefs.mspx

How to Use Sysprep: An Introduction
http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/introductoin.mspx

Microsoft Windows XP Hotfix Installation and Deployment Guide
http://www.microsoft.com/windowsxp/downloads/updates/sp1/hfdeploy.mspx

NTFS vs. FAT: Which Is Right for You?
http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.mspx

Predefined Security Templates
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/
sag_scedefaultpols.mspx

Remote Installation Services
http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/enus/
prbc_cai_byil.asp

Securing Wireless LANs with Certificate Services
http://www.microsoft.com/technet/security/prodtech/win2003/pkiwire/swlan.mspx

Securing Wireless LANs with PEAP and Passwords
http://www.microsoft.com/downloads/details.aspx?FamilyID=60c5d0a1-9820-480e-aa38-

63485eca8b9b&displaylang=en

Set Up and Use Internet Connection Sharing
http://www.microsoft.com/windowsxp/using/networking/learnmore/ics.mspx

Step-by-Step Guide to Internet Protocol Security (IPSec)
http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp

Stored User Names and Passwords Overview
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/key_concepts_overview.mspx

Strengthening Key and File Security
http://www.microsoft.com/resources/documentation/windows/xp/all/reskit/enus/prnb_efs_mjtv.asp

Universal Plug and Play in Windows XP
http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/upnpxp.mspx

Using Software Restriction Policies to Protect Against Unauthorized Software
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx

Using Windows XP Professional with Service Pack 1 in a Managed Environment: Remote Assistance
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/22_xprem.mspx

Well-Known Security Identifiers
http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/enus/prnc_sid_cids.asp

Wi-Fi
http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

Windows Security Center—Managing the State of Security
http://www.microsoft.com/windowsxp/sp2/wscoverview.mspx

Windows Server 2003 System Services Reference
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/techref/sptcgsss.mspx

Wireless XP Wireless Auto Configuration: The Cable Guy, November 2002
http://www.microsoft.com/technet/community/columns/cableguy/cg1102.mspx

Windows XP Wireless Deployment Technology and Component Overview
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx

B.6.5 Knowledge Base Articles

Article 217098, *Basic Overview of Kerberos User Authentication Protocol in Windows 2000*
http://support.microsoft.com/?id=217098

Article 254649, *Overview of Memory Dump File Options for Windows 2000, for Windows XP, and for Windows Server 2003*

http://support.microsoft.com/?id=254649

Article 279765, *How to Use the Fast User Switching Feature in Windows XP*
http://support.microsoft.com/?id=279765

Article 282784, *Qfecheck.exe Verifies the Installation of Windows 2000 and Windows XP Hotfixes*
http://support.microsoft.com/?id=282784

Article 294739, *A Discussion About the Availability of the Fast User Switching Feature*
http://support.microsoft.com/?id=294739

Article 296861, *How to Install Multiple Windows Updates or Hotfixes with Only One Reboot*
http://support.microsoft.com/?id=296861
Article 304040, *How to Configure File Sharing in Windows XP*
http://support.microsoft.com/?id=304040

Article 307973, *How to Configure System Failure and Recovery Options in Windows*
http://support.microsoft.com/?id=307973

Article 308422, *How to Use Backup to Back Up Files and Folders on Your Computer in Windows XP*
http://support.microsoft.com/?id=308422

Article 309340, *How to Use Backup to Restore Files and Folders on Your Computer in Windows XP*
http://support.microsoft.com/?id=309340

Article 310749, *New Capabilities and Features of the NTFS 3.1 File System*
http://support.microsoft.com/?id=310749

Article 314343, *Basic Storage Versus Dynamic Storage in Windows XP*
http://support.microsoft.com/?id=314343

Article 314834, *How to Clear the Windows Paging File at Shutdown*
http://support.microsoft.com/?id=314834

Article 314984, *How To Create and Delete Hidden or Administrative Shares on Client Computers*
http://support.microsoft.com/?id=314984

Article 320820, *How to Use the Backup Utility to Back Up Files and Folders in Windows XP Home Edition*
http://support.microsoft.com/?id=320820

Article 322389, *How to Obtain the Latest Windows XP Service Pack*
http://support.microsoft.com/?id=322389

Article 330904, *Messenger Service Window That Contains an Internet Advertisement Appears*
http://support.microsoft.com/?id=330904

Article 810207, *IPSec Default Exemptions Are Removed in Windows Server 2003*
http://support.microsoft.com/?id=810207

Article 837243, *Availability and Description of the Port Reporter Tool*
http://support.microsoft.com/?id=837243

Article 832017, *Service Overview and Network Port Requirements for the Windows Server System*
http://support.microsoft.com/?id=832017

Article 875352, *A Detailed Description of the DEP Feature in Windows XP Service Pack 2*
http://support.microsoft.com/?id=875352

Article 890830, *The Microsoft Windows Malicious Software Removal Tool*
http://support.microsoft.com/?id=890830

Article 893357, *The Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) Update for Windows XP with Service Pack 2 Is Available*
http://support.microsoft.com/?id=893357

Article 894193, *How to Obtain and Use the Enterprise Update Scan Tool*
http://support.microsoft.com/?id=894193

B.7 Other Web-Based Resources

How Windows Server 2003's Software Restriction Policies Improve Security
http://www.windowsecurity.com/articles/windows_2003_restriction_policies_security.html

National Industrial Security Program Operating Manual, DoD 5220.22-M, by the Department of Defense
http://www.dss.mil/isec/nispom.pdf

National Security Agency Security Recommendation Guides for Windows XP
http://nsa2.www.conxion.com/winxp/

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, by the Department of Justice
http://www.cybercrime.gov/s&smanual2002.htm

Windows XP Resource Center
http://labmice.techtarget.com/windowsxp/default.htm

Windows XP Service Pack 2 Beta First Look, by Kurt Hutchinson
http://arstechnica.com/reviews/os/sp2-beta.ars/1

WinXPnews
http://www.winxpnews.com

Appendix C

Desktop Security Best Practices

The Security Best Practices outlined below have been collected from numerous recommendations and suggestions from Security experts and Microsoft. They are provided as quick reference for IT Administrators looking for a concise list of Best Practices.

C.1 Preliminary Security Steps

1. Conduct a risk assessment: See NIST SP 800-30

2. Develop a comprehensive organizational Desktop Security Policy, get management buy-in, and have the power and tools to enforce it.

3. Select and customize a security configuration baseline and lock it down with automated enforcement: Microsoft/NIST High Security templates.

4. Publish your security manual and train all users (CEO on down) on the policies. Explain why and how they will be enforced.

5. Prepare for Audits: *Reduce the Subjectivity of the Auditor!!!* Have a published security manual with clear, established policies and processes, the right tools, trained IT personnel and end users, and logging and reporting procedures and tools.

C.2 General Best Practices

1. Keep operating system patches up to date.

2. Install antivirus and spyware software and configure.

3. Install vulnerability scanning software and configure.

4. Keep all software updated/patched (Office XP, Internet Explorer, etc.).

5. Enable personal desktop firewall.

6. Train users on the risks of email attachments.

7. Ban peer-to-peer file sharing programs.

8. Ban desktop search tools that store company information outside your network.

9. Control or filter Web access.

10. Control/Ban storage devices on desktops.

11. Control/Ban instant messaging use.

12. Don’t use wireless networks. If you do, employ the latest standards and invest in a wireless intrusion detection and location solution.

13. Enforce strict passwords standards and change them at least every 90 days.

14. Perform regular scheduled backups.

15. Consider file/disk encryption software for laptop/mobile users.

16. Remote Access:

- Set up a DMZ
- Use VPNs
- Use 2 factor (token) authorization
- Set up a quarantine server
- Ban remote desktop and peer-to-peer file sharing applications
- Use file/disk encryption software
- Disable wireless network applications
- Conduct security policy check (AV, FW, Patch, Spyware, VPN client) before granting network access (Microsoft NAP, Cisco NAC)

C.3 Windows XP Security Tips

1. Use NTFS on all your hard drive partitions.

2. Disable Simple File Sharing.

3. Use passwords on all user accounts.

4. Use the Administrator Group with care.

5. Disable the Guest Account.

6. Use a firewall if you have a full time internet connection.

7. Use a router instead of ICS (remote users).

8. Use software restriction policies.

9. Limit the number of unnecessary accounts.

10. Rename the Administrator account.

11. Consider creating a dummy Administrator account.

12. Replace the "Everyone" group with "Authenticated Users" on file shares.

13. Prevent the last logged-in user name from being displayed.

15. Make sure that Remote Desktop is disabled.

16. Enable EFS (Encrypting File System).

17. If you use offline folders, encrypt the local cache.

18. Encrypt the Temp folder.

19. Clear the page file at shutdown.

20. Enable auditing on your workstations.

21. Disable default shares.

22. Disable dump file creation.

23. Disable the ability to boot from a floppy or CD-ROM on physically unsecured systems.

24. Disable AutoRun for the CD-ROM.

25. Consider implementing IPSec.